NISHIMURA & ASAHI

西村あさひ法律事務所

オンライン上の外部攻撃と事業継続対応

事業再生/倒産ニューズレター　2022 年 2 月 28 日号

執筆者:
E-mail 柴原 多

1. はじめに

法人は、事業継続することにより、その存続目的を実現することが最重要課題であるが、数々のリスクによって、当該目的の実現が阻害されることが少なくない[1]。

伝統的には、財務状態の悪化やコンプライアンス違反が阻害事由となってきたが、2020 年からは COVID-19 が重大な阻害事由として挙げられるようになった。これを受けて人々は、より一層オンライン社会の重要性を認識したが、他方で同社会における阻害事由としてはオンライン上の外部攻撃(以下単に「外部攻撃」という)が挙げられる[2]。

実際、報道によると[3]、2016 年以降国内で少なくとも 11 の病院がランサムウェアによる被害を受けているとのことであり[4]、米国では当該被害を原因として連邦倒産法第 11 章(通称「チャプター11」)の適用を申請している企業も存在する。

そこで以下では、外部攻撃が企業に与える影響及びその留意点について言及していく。

2. オンライン環境の重要性とリスク

多くの人が実感しているとおり、現代社会はオンライン環境なくしては生活できない社会となりつつある。この流れは、コロナ禍において、リモートワークの普及により加速化すると共に、デジタルトランスフォーメーション(DX)の流れ[5]とも歩調を合わせていくこと

---

1 企業が(阻害事由からの)事業復元力を適切に発揮するには、事業継続計画(Business Continuity Planning(以下「BCP」という)に基づき事業継続対応を行うことが重要である。ここでいう BCP とは本来、緊急事態発生時に、企業が損害を最小限に抑え、事業の継続や復旧を図るための計画のことをいう(例えば、中小企業庁 HP「中小企業 BCP 策定運用指針」https://www.chusho.meti.go.jp/bcp/contents/level_c/bcpgl_01_1.html 参照のこと)。

なお当該 HP においては The Business Continuity Institute の提言を参考にして①優先して継続・復旧すべき中核事業の特定、②緊急時における目標復旧時間の設定、③緊急時に提供できる役務の程度について協議、④事業拠点、生産設備、仕入品調達等の代替策の用意、⑤従業員と事業継続についてコミュニケーションを図っておくこと、が BCP の特徴として記載されている。

2 特に政府が重要インフラと指定する 14 分野にとって外部攻撃の影響は甚大である点に留意が必要である(内閣サイバーセキュリティセンターHP「重要インフラの情報セキュリティ対策に係る第4次行動計画」https://www.nisc.go.jp/active/infra/outline.html 参照のこと)。

3 詳細は、読売新聞 2021 年 12 月 29 日付記事参照のこと。なお 2021 年の世界全体での攻撃は 2845 件と報告されており、日本国内における 2021 年上半期の状況は警察庁 HP「令和3年上半期におけるサイバー空間をめぐる脅威の情勢等について」https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf 参照のこと。なお同 HP では二重恐喝(暗号化したデータへの金銭要求と窃取したデータ公開への金銭要求)についても言及されている。

4 報道によると、外部攻撃を受けた半田病院(徳島)は新システムの構築に 2 億円投じたとのことである(https://www.j-cast.com/trend/2021/12/04426315.html?p=all)。またこの他にも報道によると、2021 年 7 月に外部攻撃を受けた企業 A は四半期報告書の提出も 3 ヶ月程延期し、2021 年 8 月に外部攻撃を受けた企業 B は 6.5 億円の特別損失を計上したとのことである。

5 ①企業におけるコスト削減要請、②消費者への迅速なサービス提供に加え、③経営陣としてはデータ収集・分析に基づく(経営への)透明性の確保への要望は避けがたいものがあるとされる。

になる[6]。

他方で、人々がオンラインに依存すればする程、前述のとおり外部攻撃がなされるリスクも増加し、この問題は個人情報漏洩(現に近時も大手企業における情報管理のあり方が問題となっている)や内部統制の問題のみならず、企業の存続にも影響を与えかねない。

3. 外部攻撃の具体例

(1) 日本における具体例

まず、外部攻撃が原因で企業が破綻に至ったものとしては、マウントゴックス事件が有名である。この事件は、会社に対する外部攻撃がなされた後、顧客へのビットコインの返還が困難となり、2014 年 4 月に破産手続が開始された。その後、(ビットコインの価格高騰等の事情もあり)債権者の意向を踏まえて民事再生手続に移行し、2021 年 10 月に認可決定に至った。この事件に関しては代表者が起訴され、執行猶予付きの有罪判決が出されると共に、海外でハッカーが逮捕されているが、2021 年 12 月現在、事件の真相は少なくとも外部には明らかにされていない。

次に国内では、2018 年 1 月に発生したコインチェック事件が有名である。この事件も、仮想通貨の流出が発生し、金融庁による業務改善命令が 2 度出され、結果として(同年 4 月に)マネックスグループ株式会社による完全子会社化によって終結を見たものである。

この二つの事件はいずれも仮想通貨に絡む事件であるが、外部攻撃の影響は仮想通貨以外の事業を営む会社でも十分に発生しうる点に留意が必要である。

(2) 米国における具体例

例えば米国で破綻に至った事件としては、医療費回収機関である American Medical Collection Agency 事件(データ流出が発生し約 2000 万人が影響を受けたとされる)があり、2019 年 6 月にチャプター11 を申請するに至っている[7]。

更に 2021 年 5 月には、米パイプライン最大手のコロニアル・パイプラインが、サイバー攻撃を受けて操業停止に至っている[8]。

(3) 日本政府の対応

コロニアル・パイプライン事件は、日本の内閣サイバーセキュリティセンターの関心も喚び「ランサムウエアによるサイバー攻撃に関する注意喚起について」との情報発信がなされている[9]。具体的には、①ランサムウェアの感染を防止するための対応策、②データの暗号化による被害を軽減するための対応策、③不正アクセスを迅速に検知するための対応策、④迅速にインシデント対応を行うための対応策、の 4 つが提唱されている。

4. 緊急事態対応

(1) 事業継続対応

では、仮に外部攻撃によって業務に重大な支障が生じた場合、事業継続のために、経営者はどのような対策を講じるべきであろうか[10]。

---

6 データ分析による透明性の確保と法務部の役割については、例えば、Cornelius Grossmann (EY Global Law Leader) (2021) "The General Counsel Imperative: How do you turn barriers into building blocks?"https://www.ey.com/en_gl/law/general-counsel-imperative-barriers-building-blocks 参照のこと。

7 例えば、Charlie Osborne (2019) "Data breach forces medical debt collector AMCA to file for bankruptcy protection"https://www.zdnet.com/article/medical-debt-collector-amca-files-for-bankruptcy-protection-after-data-breach 参照のこと。

8 詳細は Richard Beales「米パイプライン攻撃、インフラ脆弱性への最大の警告」(ロイター2021 年 5 月 11 日)https://jp.reuters.com/article/breakingviews-us-pipelines-idJPKBN2CS08J 参照のこと。なお日本での文献としては山岡裕明「経営判断を迫るサイバー攻撃・ランサムウェアの最新動向について」国際商事法務 2021 年 10 月号参照のこと。

9 具体的には、内閣サイバーセキュリティセンター「ランサムウエアによるサイバー攻撃に関する注意喚起」https://www.nisc.go.jp/active/infra/pdf/ransomware20210430.pdf 参照のこと。

10 なお如何に事業を継続させるかという問題とは別に、どのタイミングで捜査機関に相談するかという問題も存在する。

第一に、当該支障が何時から発生するのか、既発生なのかを確認する必要がある。

第二に、当該支障は短期に回復可能か、長期の影響が生じるかを確認する必要がある。

第三に、いずれの場合であったとしても、顧客又は関係者(現実には業務委託先等を含み、この関係者の定義も問題となるが、以下では単に「顧客等」という)に対する連絡[11]及び顧客に損害が生じない様な体制作り[12]が不可欠となる。

第四に、被害の状況によっては対外的な公表方法も検討の対象となる[13]。

第五に、以上のような体制を構築するために資金の確保も必要となる場合もある[14]。

第六に、緊急事態対応に必要なデータが会社からアクセス可能であれば、スムーズな対応もできようが、データ自体がアクセス困難となる場合にはバックアップをとっているか、そのバックアップが安全に保管されているか(場合によってはその保管場所の適否も問題となりうる)が問題となる。

第七に、緊急事態対応が終わった場合でも、顧客等に損害が生じた場合には、当該補填を行うかどうかが検討の対象となる[15]。

第八に、外部攻撃がランサムウェアの場合に相手方と交渉を行うかは(善管注意義務に関連する)非常に悩ましい問題(特に病院等がターゲットとされた場合には患者の生命等に影響を及ぼす結果ともなりかねない)であり、性質上、その全てが公表されるものでもない[16]。またこの点に関して、米国においては 2020 年 10 月 1 日、金融機関や保険会社等が被害者に代わってランサムウェアに関する身代金を支払った場合、財務省外国資産管理室(OFAC)の規制に違反するリスクがある旨が指摘されている点にも留意が必要である[17]。

(2) 事業継続計画

このような事業継続対応は、前提として適切な BCP を作成できるかどうかとも関係する。例えば、COVID-19 の場合は、当該疫病により売上に如何なるダメージが生じるかの把握、いつ売上が回復するかの見通し、その回復の期間までの体制維持、資金確保、顧客対応、従業員対応等が BCP として必要となる[18]。

この問題は外部攻撃においても同様であり、前述したように如何に外部攻撃を認識するか、外部攻撃の種類に応じた対応ができているか、当該攻撃により如何なるダメージが生じるかの把握、いつ売上が回復するかの見通し、その回復の期間までの体制維持、資金確保、顧客対応、従業員対応等が肝要である。

この点、経済産業省は「サイバーセキュリティ経営ガイドライン Ver2.0」を公開している[19]。

当該ガイドラインは、①サイバーセキュリティの対応方針策定、②リスク管理体制の構築、③資源(予算・人材等)の確保、④リスクの把握と対応計画策定、⑤保護対策(防御・検知・分析)の実施、⑥PDCA の実施、⑦緊急対応体制の整備、⑧復旧体制の整備、⑨サプライチェーンセキュリティ対策、⑩情報共有活動への参加、を提言しているが、概要は以下のことを述べているものと理

---

11 全員に連絡できるか、全員が困難であれば、如何なる範囲で、如何なる方法で連絡できるのかを検討することになろう。

12 顧客に対するサービス提供は平常時と同様に行えるのか、行えないとするなら如何なる方法なら行えるか、又自分では行えない場合に第三者による提供は可能かを検討することになろう。

13 適時開示の問題もあるが、顧客戦略的に開示するべきかの検討も重要になる。

14 当然のことながら資本調達の時間もないため、金融機関から資金を調達できるか、その際の担保は存在するのか、或いは資産売却によって資金を確保できるのかを見極める必要がある。

15 取引先との契約関係については、例えば、山岡裕明「ランサムウェアへの感染被害により生じる取引先への契約責任と不可抗力条項の定め方」https://www.businesslawyers.jp/practices/1400 参照のこと。

16 実務的には企業の加入している保険が、ランサムウェアに関する身代金を保険金の支払対象にしているかが重要であり、日本においては対象外であることが多いとの指摘もある。

17 具体的には、The U.S. Department of the Treasury (2020)"Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf 参照のこと。但し、実際には当該制裁の対象行為は限定されているとされる。米国の状況の詳細については新井敏之他「脅威型サイバー攻撃の現状と企業対応の実務」会社法務 A2Z 2021 年 5 月号参照のこと。

18 東日本大震災との関係であるが、内閣官房情報セキュリティセンター(現在の内閣サイバーセキュリティセンター)がまとめたものとしては「IT-BCP 策定モデル」(2013 年 6 月)https://www.nisc.go.jp/active/general/pdf/IT-BCP.pdf 参照のこと。

19 具体的には、経済産業省 HP「サイバーセキュリティ経営ガイドライン」https://www.meti.go.jp/policy/netsecurity/mng_guide.html 参照のこと。

解できる。

すなわち、企業の目的である利益確保のためには、投資、特に IT 投資が重要であるが、それと同時に IT の防御力も重要性を増し、それによってステークホルダーの信頼も確保されることとなる。勿論、企業としては無制限にコストをかける訳にはいかず、対応しきれないリスク(残留リスク)も存在するが(いざという時のためには)当該リスクを認識しておくことが重要である。

また、リスクへの完全な対応は存在しえないため、①多層に亘る防御と教育が重要であること、②リスクの変化に対応するには PDCA の実施及び BCP との連携が重要であること、に留意が必要であるといえよう[20]。

なお、かかる体制の構築に際して注意を要するのは、新規の外部事情による被害は、関係者から比較的理解のある反応がなされることが多いが、同種の被害が増加する傾向にあればある程、予想されるトラブルへの準備不足への非難の色合いが強まってくる点である。

(3) 責任の所在

また仮に緊急事態が解決したとしても、その原因解明・責任対応の検討は、今後の企業運営にとって不可欠な課題となる。当然のことであるが、原因が解明されなければ第二、第三の危機が到来する可能性があり、また当該危機が不可抗力によるものであるかはステークホルダーとしても重要な関心を寄せることが多いからである。

この原因解明については、専門家の協力が不可欠な場合があるが、原因が高度化すればする程その解明は困難になると共に、コスト見合いも重要なテーマとなってくる[21]。

更に責任対応については、保険の利用[22]のみならず、善管注意義務に配慮した体制作り、簡単に言えば①業界上の標準を踏まえた組織体制を構築していたか、②不正行為を予見できるような特段の事情は存在しなかったかの検証が必要となる[23]。

すなわち、現代社会における IT の重要性・リスクを踏まえると、IT 上の攻撃に対する防御体制の構築は善管注意義務の内容たる内部統制に該当し、少なくとも取締役には業界標準の注意を払うべきとの義務が課されると共に、仮に標準以上の義務は履行していたとしても、損害を発生させるような不正行為を認識できるような特段の事情が存在する場合には、当該不正行為を防止すべきとする義務もまた課される可能性があるからである。

5. 結語

以上述べたとおり、企業は不測の事態の全てに対応することは困難である。しかしながら、不測の事態に適切に対応し、事業継続上の疑念を払拭することは非常に重要な使命でもある。そして、不測の事態への対応及び対応方法の策定は、トライ&エラーを踏まえた検証に尽きるが、当該検証に際しては先例、各団体の出しているガイドライン等の情報収集及び自己の事業の弱点を把握し、不断の努力を積み重ねることにより、少なくとも業界標準以上の体制を構築していく必要がある。

西村あさひ法律事務所 広報室 E-mail

---

20 企業が責任を最小化する方法としては、例えば、髙取芳宏他「ランサムウェア：進化するサイバー脅威に企業はどう備えるべきか、どのように『証拠』を残すべきか。」JCA ジャーナル 2018 年 1 月号参照のこと。

21 コストを無制限にかけることは企業の存在目的とも反する可能性がある点に留意が必要である。

22 前述のガイドラインでも言及されている。なお、サイバー賠償保険におけるランサムウェアの割合に関しては、Coalition, Inc. “Cyber Insurance Claims Report (H1 2021)”https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2021-07-Coalition-Cyber-Insurance-Claims-Report-2021-h1.pdf 参照のこと。

23 なお参考になる判例の分析については、塩崎彰久他『サイバーセキュリティ法務』(2021 年、商事法務)18 頁以下参照のこと。